Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES
SERVICE DES SYSTÈMES D'INFORMATION
Sous-direction de la production
Bureau des infrastructures et des outillages – SI-2B
4 avenue Montaigne
93 468 NOISY-LE-GRAND Cedex
Affaire suivie par Bruno Lécrivain
✉ bruno.lecrivain@dgfip.finances.gouv.fr
☎ 01 57 33 75 34

Paris, le 15 avril 2020

Fiche technique

Objet : Campagne IR – ouverture de E-contacts derrière le PIGP : sécurité informatique

Important : les consignes ci-dessous s'appliquent exclusivement aux agents utilisant le PIGP. Les agents disposant d'un matériel de travail à distance avec VPN doivent utiliser leur connexion VPN, plus sécurisée. En particulier, un utilisateur de VPN ne doit pas changer son mot de passe pendant la crise, au risque de ne pas pouvoir se reconnecter à son ordinateur fixe. Les principes généraux de vigilance sont néanmoins d'intérêt commun.

L'ouverture de l'accès à E-contacts à travers le portail internet de la gestion publique (PIGP) présente un enjeu extrêmement fort de sécurité informatique et de préservation de la confidentialité des échanges avec les usagers.

En effet, le PIGP est ouvert sur Internet : toute personne qui dispose d'un nom d'utilisateur DGFiP et de son mot de passe, parfois rudimentaire, peut y accéder ainsi qu'aux applications ouvertes et aux informations qu'elles contiennent, là où en temps normal il faut préalablement être connecté au réseau DGFiP avec un ordinateur DGFiP, protégé, pour pouvoir accéder à l'application.

En conséquence, certaines mesures doivent être mises en place pour limiter les risques :

– accéder au PIGP et à E-contacts toujours depuis le même ordinateur, avec le même accès internet et sans utiliser de VPN personnel ou d'autre dispositif d'anonymisation ;

– l'ordinateur utilisé devra fonctionner sous Windows 10 : les versions de Windows antérieures (comme Windows 7 ou Windows Vista) souffrent de failles de sécurité graves qui ne sont plus corrigées ; leur utilisation pour accéder à E-contacts au travers du PIGP est proscrite ; il en est de même des systèmes alternatifs (Linux, Mac, tablettes, smartphones…) dont l'utilisation dans ce cadre n'est pas validée ;

– s'assurer que le système d'exploitation est à jour de toutes les mises à jour (« Tous les paramètres » > « Mise à jour et sécurité » > « Rechercher des mises à jours ») ;

– avoir un antivirus et un pare-feu à jour et activés sur le poste : sous Windows 10 vous êtes par défaut protégé par l'antivirus et le pare-feu de Windows, sauf si vous avez installé un antivirus tiers (qui en général intègre un pare-feu, ce que vous devrez vérifier) ou si vous avez désactivé manuellement l'antivirus ou le pare-feu (auquel cas, il faut les réactiver) ;

– créer sur votre PC personnel un compte utilisateur standard (non administrateur) dédié pour accéder à e-contact au travers du PIGP (« Tous les paramètres » > « Comptes » > « Famille et autres utilisateurs » > « Ajouter un autre utilisateur sur ce PC » > « Je ne dispose pas des informations de connexion de cette personne » > « Ajoutez un utilisateur sans compte Microsoft » > Saisissez un nom d'utilisateur (par exemple *pnom*_travail) et un mot de passe ;

– se connecter sous ce compte pour vos séances de travail sur le PIGP (si nécessaire, redémarrer l'ordinateur et sélectionner votre nouveau compte en bas à gauche de l'écran de connexion) ;

– utiliser le navigateur Edge mis à jour avec le système d'exploitation Windows 10 ;

- toujours vérifier que l'adresse lors de la connexion au PIGP est bien : https://portail.dgfip.finances.gouv.fr/portail/accueilIAM.pl
- lorsque le navigateur Edge propose de « Laisser Microsoft Edge enregistrer et entrer vos mots de passe pour ce site la prochaine fois », sélectionner « Jamais » ;
- utiliser un mot de passe sécurisé et protégé pour votre connexion au PIGP :
  - de 12 caractères combinant minuscules, majuscules et chiffres :
    - les recommandations sont disponibles dans l'aide de l'interface de changement de mot de passe : https://portail.dgfip.finances.gouv.fr/changement_mdp/oaa2/gestion-mdp/Aide-Mot_de_Passe.htm
    - lors du changement de mot de passe sur l'interface, un indicateur de robustesse est affiché, il doit être à fort ;
    - testez, sans accès au réseau DGFiP, la solidité de vos mots de passe sur la page du fonctionnaire de sécurité des systèmes d'information du ministère : https://ssi.economie.gouv.fr/motdepasse
  - le mot de passe doit être conservé secret :
    - ne pas être inscrit sur un post-it ou dans un fichier sur le disque dur ;
    - ne pas être saisi sur une page dont on n'est pas sûr de la fiabilité (l'adresse du PIGP est rappelée ci-dessus) ;
    - ne pas être utilisé sur un autre site (personnel comme professionnel) ;
    - en particulier, le hameçonnage ou phishing est une pratique classique des pirates, elle peut consister par exemple à envoyer un mail à plusieurs personnes en leur indiquant que leur mot de passe va expirer et qu'il faut le changer en cliquant sur un lien. La page qui s'ouvre alors, et qui peut ressembler beaucoup à une page légitime DGFiP, vise à capturer le mot de passe de l'utilisateur pour pouvoir ensuite usurper son identité. Si vous souhaitez/devez changer votre mot de passe, faites-le exclusivement :
      - soit en utilisant le lien « Accéder au changement de mot de passe » une fois connecté sur le PIGP (adresse ci-dessus) ;
      - soit depuis Ulysse > Assistance informatique > Messagerie (Courrielleur, mot de passe, gestion des messages d'absence…) > Changer de mot de passe ;
- si vous constatez quelque chose d'inhabituel, changer immédiatement de mot de passe et informer votre hiérarchie ainsi que la BALF : soc@dgfip.finances.gouv.fr

Vous pouvez retrouver une documentation très riche sur les bonnes pratiques à l'adresse : https://www.cybermalveillance.gouv.fr/bonnes-pratiques